

Remarks

In the interest of clarity the paragraph numbers below mirror the substantive paragraph numbers in the Advisory Action.

2a. The Advisory Action draws a distinction between “application distinct identification numbers” and “information about the patient identification number used by each application” where the latter phrase is being interpreted more broadly than the former to include the tables and indexes described in Felsher. To overcome Felsher, Applicant has amended claim 1 so that the claim 1 reference table includes a list of applications and patient identification numbers (as opposed to information about those numbers) used by the applications where at least a subset of the identification numbers are application distinct patient identification numbers.

Thus, irrespective of whether or not Felsher contemplates storing information about application distinct patient identification numbers on an exchange server, Felsher clearly fails to teach or suggest storing a list of application distinct identification numbers.

2b. The Advisory Action and the most recent Office Action indicate that the combination of a private key and an applet wrapper are used to reject the application distinct identification number limitation of claim 1. Applicant strongly traverses this rejection.

As an initial matter a summary of how Felsher teaches records are requested by a system user (i.e., a record recipient) and how the system encrypts, transmits and decrypts the records is instructive. In this regard Felsher teaches that a user (i.e., a recipient) can use a workstation 12 (see Fig. 1) to request a record associated with a specific patient from a server 3/5 that is associated with a medical information database 6. To identify a specific patient in a request, the request includes a system wide patient identification number such as a social security number or the like (see paragraph 266). When a request is received, assuming that the requesting user has the right to access

the requested record, the server 3 obtains the record and then uses a public key associated with the requesting user to encrypt the record prior to transfer (see paragraphs 220, 228, 238, 242 and 252). Because the system wide patient ID number is part of the record, the patient ID number is encrypted. The public key is recipient (i.e., system user) distinct (see paragraph 220). The encrypted record is transmitted to the recipient (i.e., the requesting user) along with an applet which is a program that is usable by the recipient's workstation to decrypt the encrypted record.

In addition to requiring the applet to decrypt the encrypted record, the recipient's workstation also requires a recipient specific or distinct private key which, as the label implies, is private or known only to the recipient's workstation. The applet is not recipient distinct – i.e., the same applet is transmitted with each encrypted record irrespective of which recipient the record is transmitted to and irrespective of which application was used to access the record). Here, the private key is associated with the recipient's computer account so that the private key "follows" the user around and is available irrespective of which workstation or other device the recipient employs to access the system.

Once the recipient's workstation receives the encrypted record and the applet, the workstation decrypts the record using the private key and the applet and uses the information in the decrypted record accordingly. Here, after decryption, the patient ID is identical to the patient ID in the original record at the server.

Thus, Felsher's private keys are only associated with system users and are not stored in a central exchange server and the applets are not application distinct (i.e., the same applet is transmitted with each transmitted record irrespective of which application is used to access the record). Because the applets are not application distinct and the private keys are not stored in an exchange server table (i.e., the private key is private), the applet and private key cannot possibly be combined to teach or suggest application distinct patient identification numbers for each application on a network in an exchange server table as required by claim 1.

In addition, Felsher's private keys are not application specific keys. To this end,

private keys are recipient (i.e., system user) specific which is different than application specific. For instance, where a first physician uses multiple different application programs to access a patient record in Felsher, the physician only has a single private key used to decrypt received records irrespective of which application program is used to access the record. As an example, where a first physician accesses a first patient record using a first application and then uses a second application to access the first patient record at a later time, each time, irrespective of which application is employed to access the record, the first physician's single private key is used to decrypt.

As another instance, where two different physicians use the same application program to access a first patient record, each physician has his own private key despite the fact that only a single application is employed to access. Thus, private keys are recipient specific and not application specific.

Therefore, private keys are recipient distinct, not application distinct, the applets are not application distinct and therefore the combination of a private key and an applet cannot possibly be application specific.

A more persuasive but yet still flawed application of Felsher to the claim 1 invention would rely on the public keys that are used to encrypt records (including uniform patient identification numbers (i.e., SS numbers) prior to transmission to recipients. To this end, Felsher teaches that separate/unique public keys are maintained by server 3 for each system user that is authorized to access system records (i.e., record recipients) (see paragraph 220). When a system user requests a record, Felsher teaches that a system server accesses the user's unique public key, uses the public key to encrypt the record and transmits the encrypted record to the requesting user. Thus, the system server maintains a list of public keys for each system user that can access system records.

Despite the fact that Felsher's public keys are maintained by a central server, the public keys suffer from the same shortcoming as the private keys described above in that the public keys are recipient specific and not application specific. For instance, assume that a physician has access to several different application programs at a

medical facility and that, at two different times, the physician uses first and second different application programs, respectively, to access a first patient record that is stored in Felsher's database 6 (see Felsher's Fig. 1). Here, according to Felsher, when the physician requests the first patient record using the first application program, server 5 uses a public key associated with the first physician to encrypt the requested record and transmits the encrypted record to the physician.

When the physician requests the first patient record using the second application program, the server 5 again uses the public key associated with the first physician to encrypt the requested record. The public key used to encrypt in this second case where a second application program is used to access the first record is the same as the public key used to encrypt in the first case where the first application program was used to access the first record. In fact, irrespective of which application program the physician uses to access the first patient record, the same public key is used to encrypt and therefore, even when encrypted, a system wide patient identification number (e.g., a SS number) will include the same information when transmitted to the first physician.

As another instance, assume that two different physicians use a single application program at different times to access the first patient record. Here, according to Felsher where public keys are recipient distinct as opposed to application distinct, despite the fact that one application program is used to access the first patient record, when the first physician accesses the first patient record the server uses a first public key associated with the first physician to encrypt the first patient record and when the second physician accesses the first patient record the server uses a second public key associated with the second physician to encrypt the first patient record and each of the encrypted records includes an encrypted patient ID that is distinct.

Thus, in short, like the private keys, Felsher's public keys are recipient (i.e., user) specific and not application specific.

Moreover, applicant adds that the encryption and decryption processes described in Felsher comprise a single application and not network applications (plural) and that, where multiple applications occur in Felsher, patient identification numbers

are uniform system wide for each patient. To this end, Felsher teaches at paragraph 266 that system wide patient identification numbers are employed such as social security numbers. To transmit patient identification numbers between application programs in a secure and private manner, those numbers, as part of a patient record, are encrypted, transmitted and decrypted. Nevertheless, patient identification numbers stored by the central server 3 prior to encryption and the identification numbers used by the end application programs after decryption are identical (i.e., may be SS numbers) and what happens in between the server and the application programs is wholly part of a single encryption/decryption program.

Turning to Moragne, Moragne fails to teach what Felsher lacks with respect to claim 1. More specifically, Moragne fails to teach or suggest a system wherein an exchange server maintains a list of applications and application specific patient identification numbers.

For all of the above reasons Applicant believes claim 1 and claims that depend there from are patentably distinct over the cited references and allowance of the same is requested.

Claim 5 includes limitations similar to the limitations of claim 1. For at least the above reasons Applicant believes claim 5 and claims that depend there from are distinct over the references cited and requests that the rejections be withdrawn.

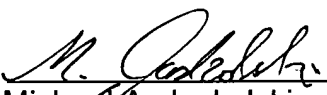
Carl Dvorak
Serial No.: 10/052,659
Office Action Response
Page 11

Applicant has introduced no new matter in making the above remarks. In view of the above remarks, Applicant believes claims 1-8 of the present application recite patentable subject matter and allowance of the same is requested. No fee in addition to the fees already authorized in this and accompanying documentation is believed to be required to enter this amendment, however, if an additional fee is required, please charge Deposit Account No. 17-0055 in the amount of the fee.

Respectfully submitted,

CARL DVORAK

Date: 3-14-07

By: 
Michael A. Jaskolski
Reg. No. 37,551
Attorney for Applicant
QUARLES & BRADY, LLP
411 East Wisconsin Avenue
Milwaukee, WI. 53202-4497
(414) 277-5711

QBMKE\6044805.1